

Fig. 1

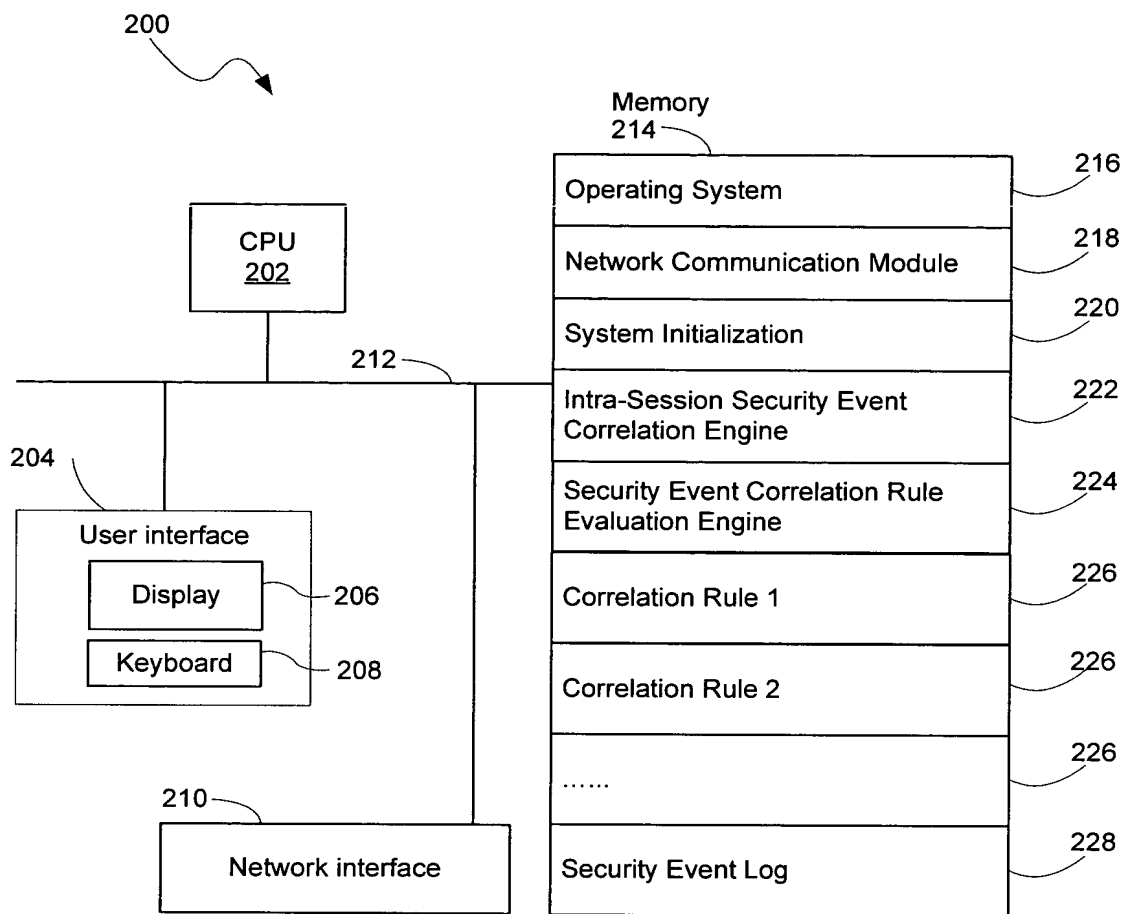


Fig. 2

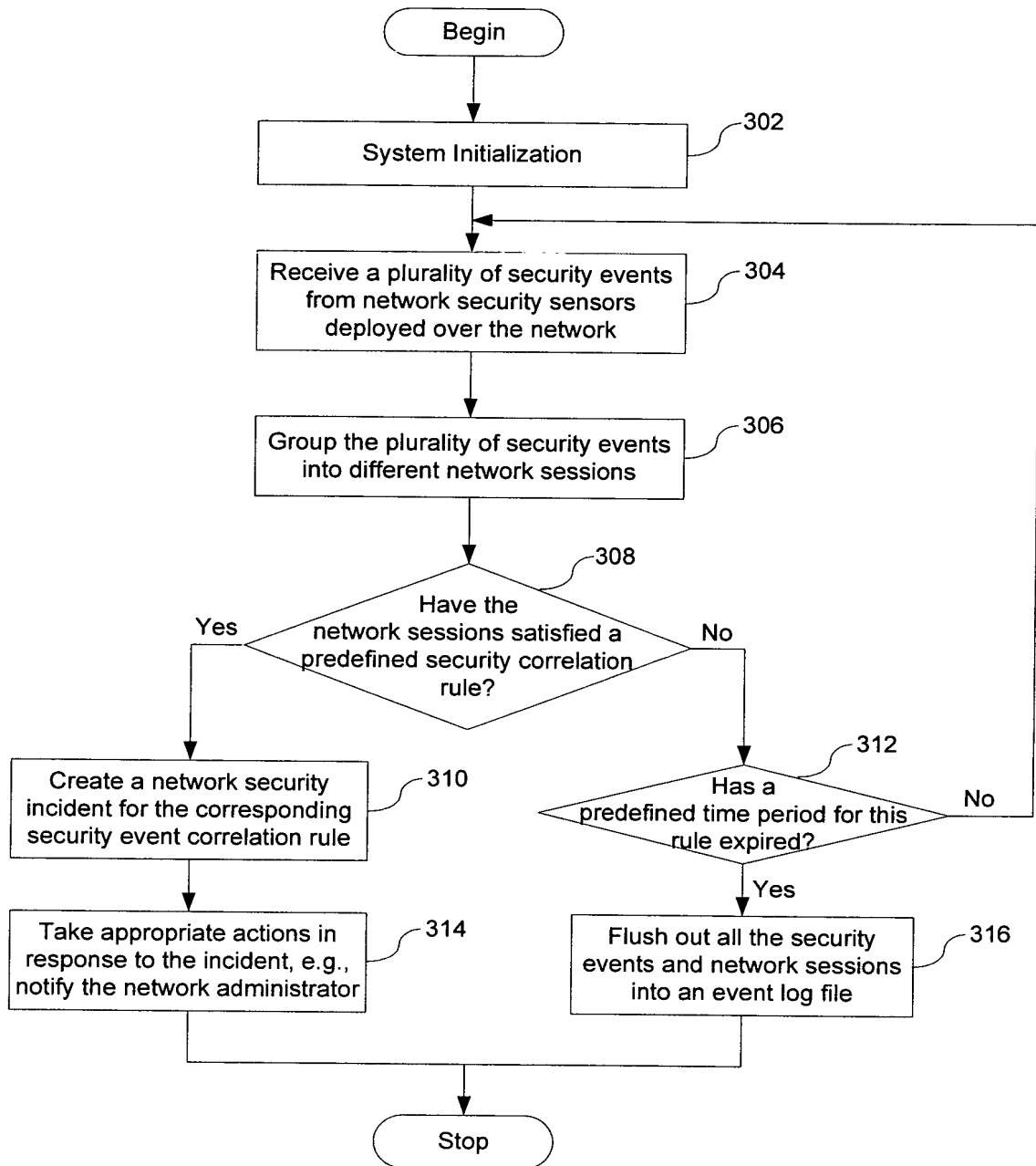


Fig. 3

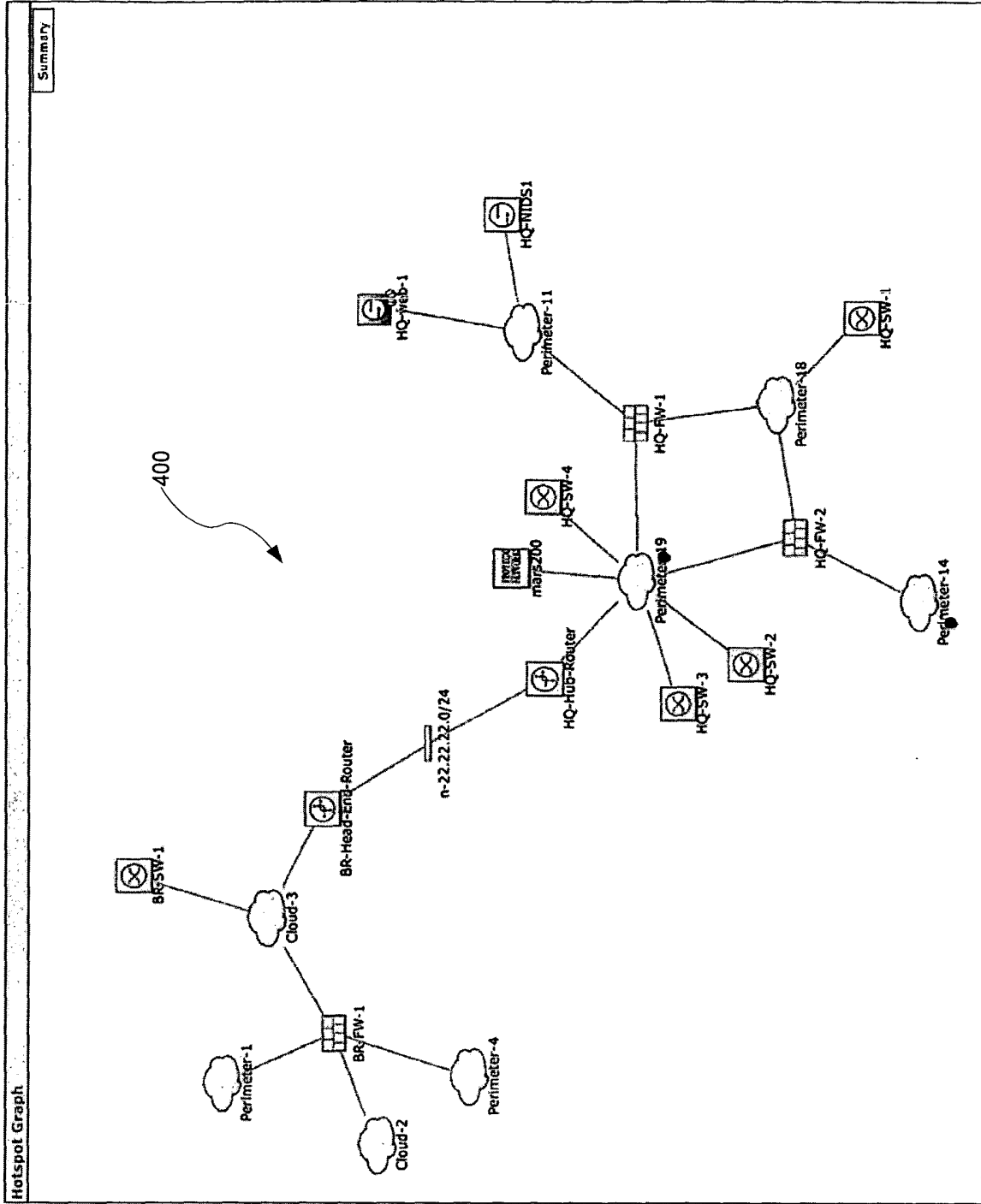
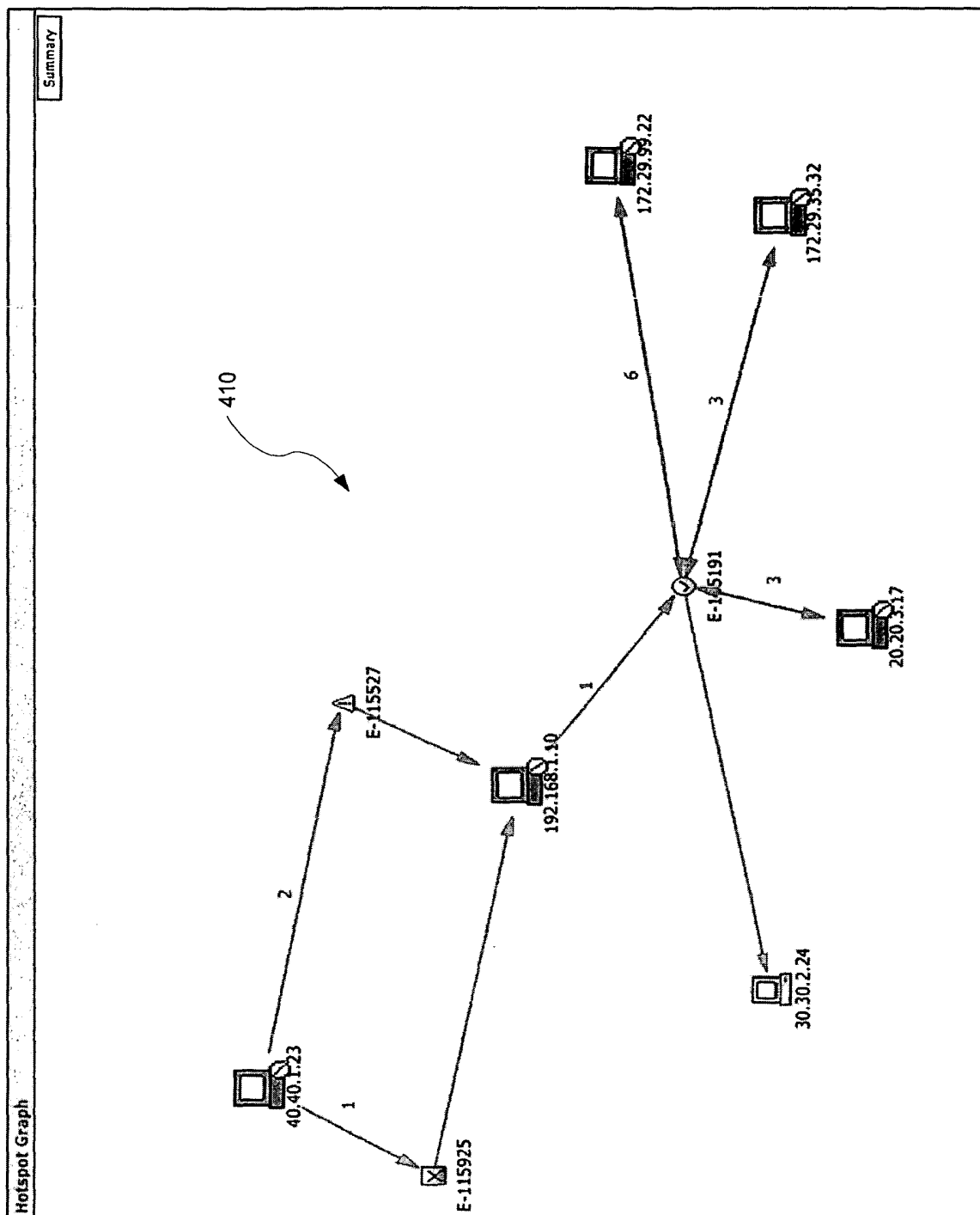


FIG. 4(A)



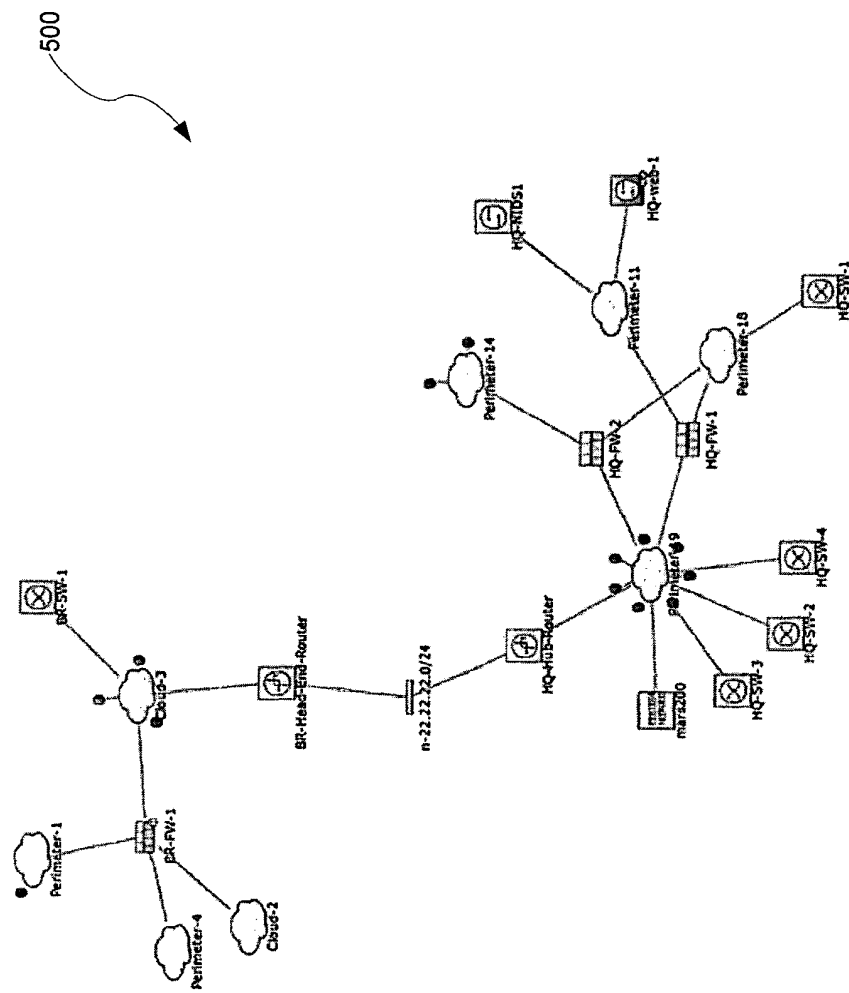
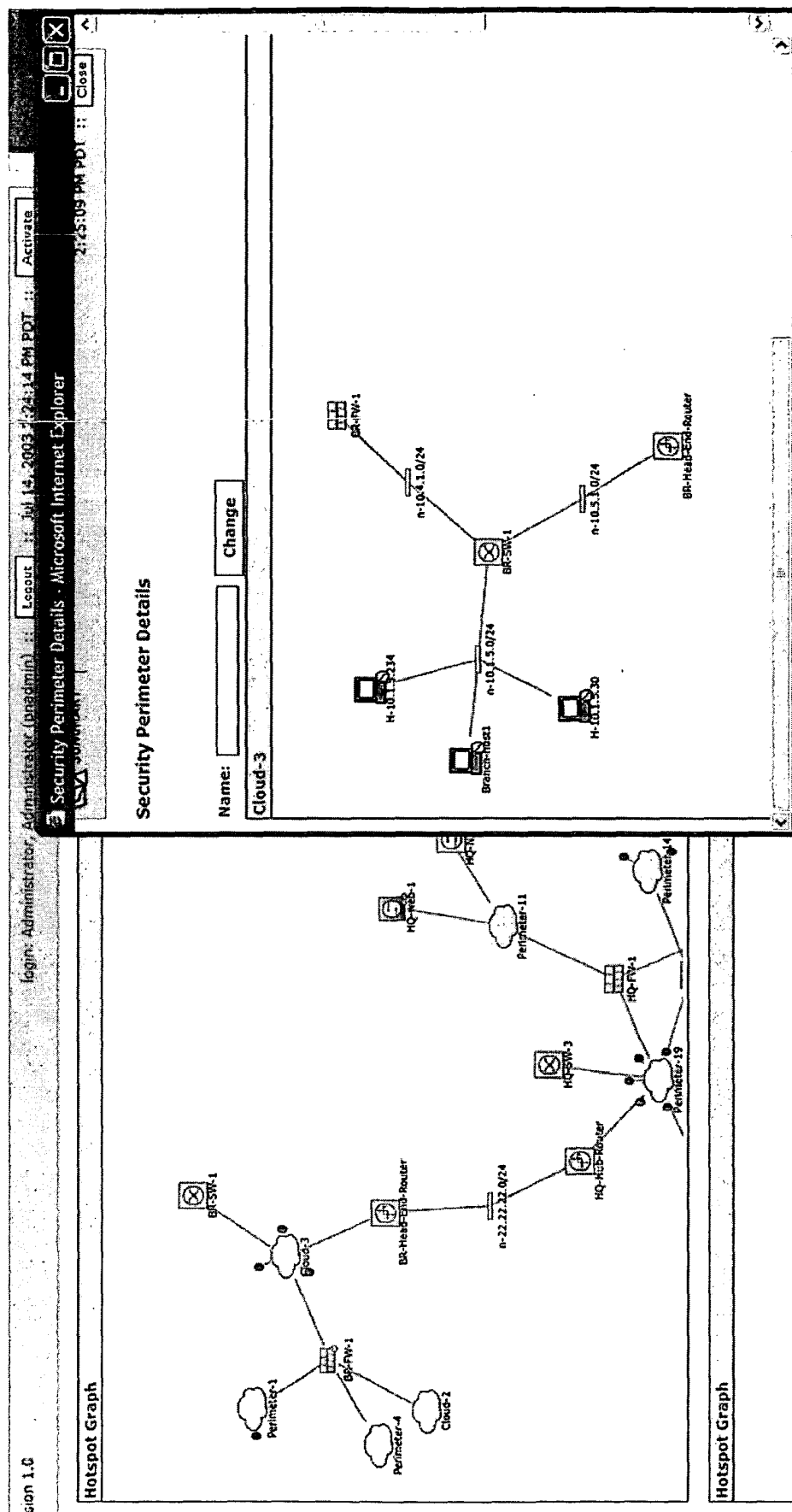


Fig. 5(A)



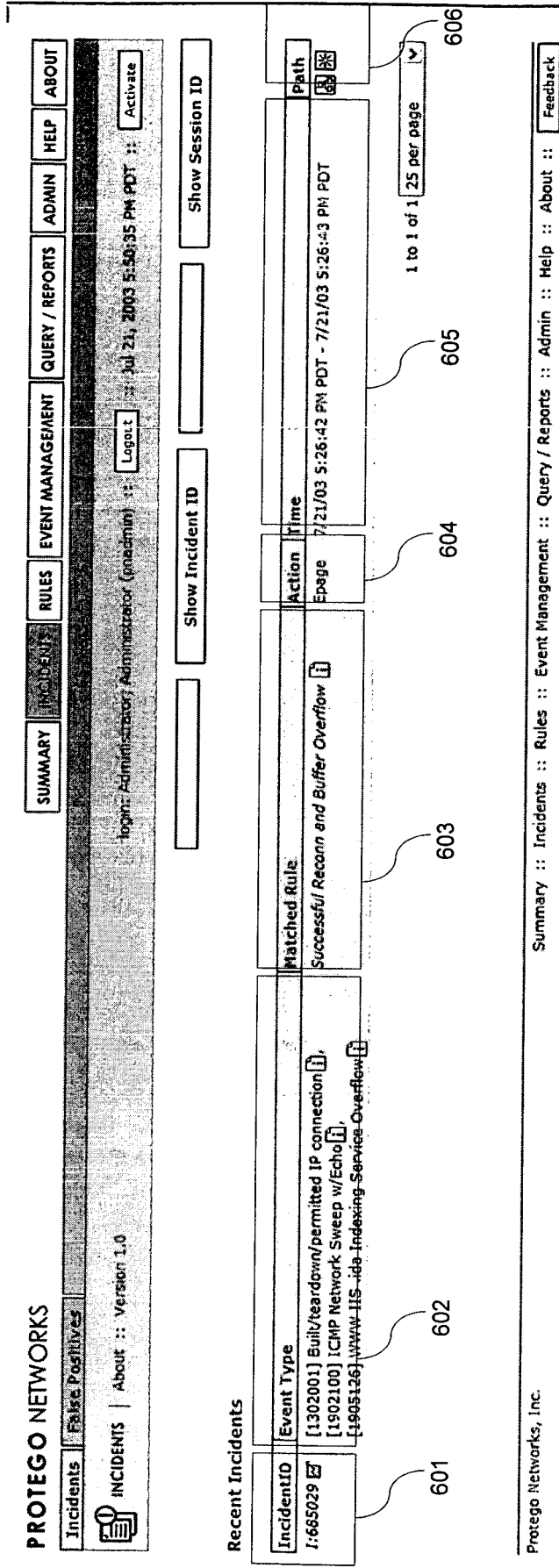


Fig. 6



# PROTEGO NETWORKS

Incidents

False Positives

INCIDENTS

About :: Version 1.0

login: Administrator, Administrator (password) :: Logout

Jul 21, 2003 5:53:45 PM PDT :: Activate

SUMMARY

INCIDENTS

RULES

EVENT MANAGEMENT

QUERY / REPORTS

ADMIN

HELP

ABOUT

685029

Show Incident ID

Show Session ID

☒ Matched Rule: Successful Recon and Buffer Overflow  
☒ Description: Successful Recon and Buffer Overflow

Offset	Open	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Zone	Action/Operation	Time-range
1		\$TARGET02	\$TARGET01	ANY	Probe/HostSweep/All	ANY	ANY	1	NY	OR	
2		\$TARGET02	\$TARGET01	ANY	Probe/PortSweep/All	ANY	ANY	1	NY	FOLLOWED-BY	
3		\$TARGET02	\$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Penetrate/BufferOverflow/FTP, Penetrate/BufferOverflow/Nail, Penetrate/BufferOverflow/RPC, Penetrate/BufferOverflow/SSH, Penetrate/BufferOverflow/Telnet, Penetrate/BufferOverflow/Web	ANY	ANY	1	NY	FOLLOWED-BY	
4		\$TARGET01	ANY	ANY	Info/AllTraffic	ANY	ANY	1	NY	Epage	0hh:5mm:0ss

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP/Port	Destination IP/Port	Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10			Total: 2				
3	S:676903 I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23	2500 192.168.1.10 80 (Executor, http, http, Web+)	TCP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1 HQ-FW-1 HQ-SW-IDSN-1			Tune
4	S:676904 I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10	2000 30.30.2.24	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1			Tune

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Fig. 7

# PROTEGO NETWORKS

Incidents

False Positives

INCIDENTS

About :: Version 1.0

login: Administrator, Administrator (padmin)

Logout :: Jul 21, 2003 5:51:45 PM PDT ::

Activate

Show Incident ID

685029

Show Session ID

Matched Rule: Successful Recon and Buffer Overflow  
 Description: Successful Recon and Buffer Overflow

Offset	Open	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Zone	Action/Operation	Time-range
1		\$TARGET02	\$TARGET01	ANY	Probe/HostSweep/All	ANY	ANY	1	NY	OR	
2		\$TARGET02	\$TARGET01	ANY	Probe/PortSweep/All	ANY	ANY	1	NY	FOLLOWED-BY	
3		\$TARGET02	\$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Penetrate/BufferOverflow/FTP, Penetrate/BufferOverflow/Http, Penetrate/BufferOverflow/RPC, Penetrate/BufferOverflow/SSH, Penetrate/BufferOverflow/Telnet, Penetrate/BufferOverflow/Web	ANY	ANY	1	NY	FOLLOWED-BY	
4		\$TARGET01	ANY	ANY	Info/AllTraffic	ANY	ANY	1	NY	Epage	0hh:5mm:0ss

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP / Port	Destination IP / Port	Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-SW-IDS-M-1			Tune
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1			Tune
3	S:676903, I:685029	[1905126] WWW IIS .ida indexing Service Overflow	40.40.1.23	2500 192.168.1.10	TCP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1, HQ-FW-1, HQ-SW-IDS-M-1			Tune
4	S:676984, I:685029	[1302001] Build/reardown/permitted IP connection	192.168.1.10	2000 30.36.2.24	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1			Tune

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Fig. 8

# PROTEGO NETWORKS

Incidents | False Positives | About :: Version 1.0

Matched Rule: Successful Recon and Buffer Overflow  
Description: Successful Recon and Buffer Overflow

Offset	Open	Source IP	Destination IP	Service Name	Event
1		\$TARGET02	\$TARGET01	ANY	Probe/HostSweep/All
2		\$TARGET02	\$TARGET01	ANY	Probe/PortSweep/All
3		\$TARGET02	\$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Penetrate/BufferOverflow/Mail, Penetrate/BufferOverflow/SSH, Penetrate/BufferOverflow/Web
4		\$TARGET01	ANY	ANY	Info/AllTraffic

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP / Port	Destination IP / Port	Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-SW-IDSM-1		Tune	
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1		Tune	
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10	TCP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1, HQ-FW-1, HQ-SW-IDSM-1		Tune	
3	S:676903, I:685029	[1905126] WWW: IIS .ida indexing Service Overflow	40.40.1.23	2500 192.168.1.10	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1		Tune	
4	S:676984, I:685029	[1302001] Build/teardown/permited IP connection	192.168.1.10	2000 30.30.2.24	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1		Tune	

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About ::

Feedback

Fig. 9

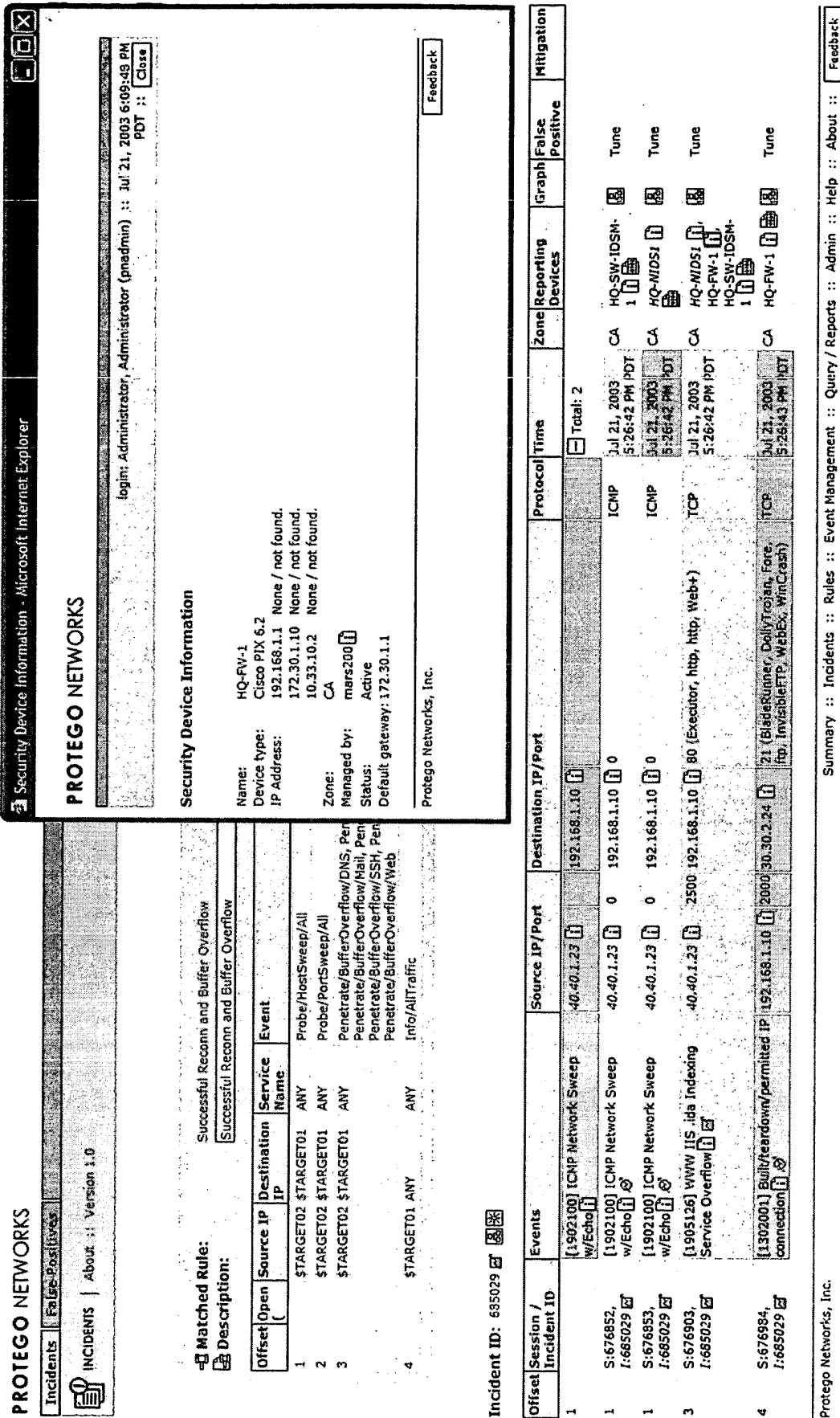


Fig. 10

SUMMARY	INCIDENTS	RULES	EVENT MANAGEMENT	QUERY / REPORTS	ADMIN	HELP	ABOUT
---------	-----------	-------	------------------	-----------------	-------	------	-------

**Activate**


 22 ELECTRONIC

Logini: Administrator, Administrator (pnædmin) :: Jul 21, 2003 5:53:50 PM PDT ::

Raw Events		ion Time-range
Event / Session / Incident ID	Reporting Device	Time
E:676852, S:676852, I:665029	HQ-SW-IDS#1	Jul 21, 2003 5:26:42 PM PDT
		40.40.1.23/0 --> 100.1.4.10/0 ICMP Network Sweep w/Echo

**Estate**

Offset	Session / Incident ID	Events	Source IP/Port	Destination IP/Port	Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1		[1902100] ICMP Network Sweep w/Echo [1]	40.40.1.23 [1]	192.168.1.10 [1]		Total: 2					
1	S:676852, I:685029 [2]	[1902100] ICMP Network Sweep w/Echo [1] [2]	40.40.1.23 [1]	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-SW-IDS-1 [1]	[2]		Tune
1	S:676853, I:685029 [2]	[1902100] ICMP Network Sweep w/Echo [1] [2]	40.40.1.23 [1]	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1 [1]	[2]		Tune
3	S:676903, I:685029 [2]	[1905126] WWW IIS_ida Indexing Service Overflow [1] [2]	40.40.1.23 [1]	2500 192.168.1.10 [1]	TCP	Jul 21, 2003 5:28:42 PM PDT	CA	HQ-NIDS1 [1], HQ-FW-1 [1], HQ-SW-IDS-1 [1]	[2]		Tune
4	S:676984, I:685029 [2]	[1302001] Build/earldown(permitted connection) [1] [2]	192.168.1.10 [1]	2000 30.30.2.24 [1]	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1 [1]	[2]		Tune

ents :	Rules :	Event Management :	Query / Donate :	Admin :	Help :	About :
--------	---------	--------------------	------------------	---------	--------	---------

[Events](#) :: [Rules](#) :: [Event Management](#) :: [Query / Reports](#) :: [Admin](#) :: [Help](#) :: [About](#) :: [Feedback](#)

 $1(A)$

PROTEGO NETWORKS

Incidents: 1 False Positives:

INCIDENTS | About :: Version 1.0

Matched Rule: Successful Recon and Buffer Overflow

Description: Successful Recon and Buffer Overflow

Offset Open Source IP Destination Service Name Event

1 \$TARGET02 \$TARGET01 ANY Probe/HostSweep/All

2 \$TARGET02 \$TARGET01 ANY Probe/PortSweep/All

3 \$TARGET02 \$TARGET01 ANY Penetrate/BufferOverflow/DNS, Penetrate/BufferOve

Penetrate/BufferOverflow/Hail, Penetrate/BufferOve

Penetrate/BufferOverflow/SSH, Penetrate/BufferOve

Penetrate/BufferOverflow/Web

4 \$TARGET01 ANY ANY Info/AllTraffic

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP/Port	Destination IP/Port
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0
3	S:676903, I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23	2500 192.168.1.10
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10	2008 50.30.2.24

Protego Networks, Inc.

Summary

Incident Graph-685029 - Microsoft Internet Explorer

PROTEGO NETWORKS

login: Administrator, Admin

Incident Graph-685029

Session ID:676852

Src: 40.40.1.23/0

Dest: 192.168.1.10/0

Event Types:

ICMP Network Sweep

w/Echo

Previous Next

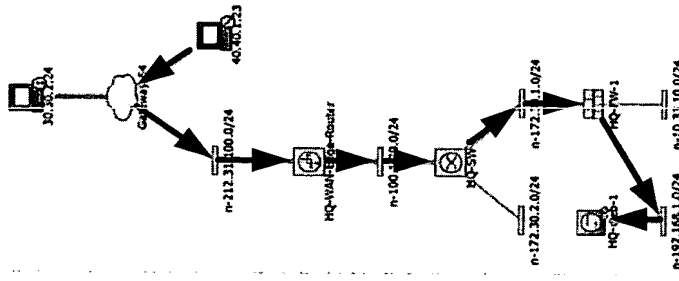
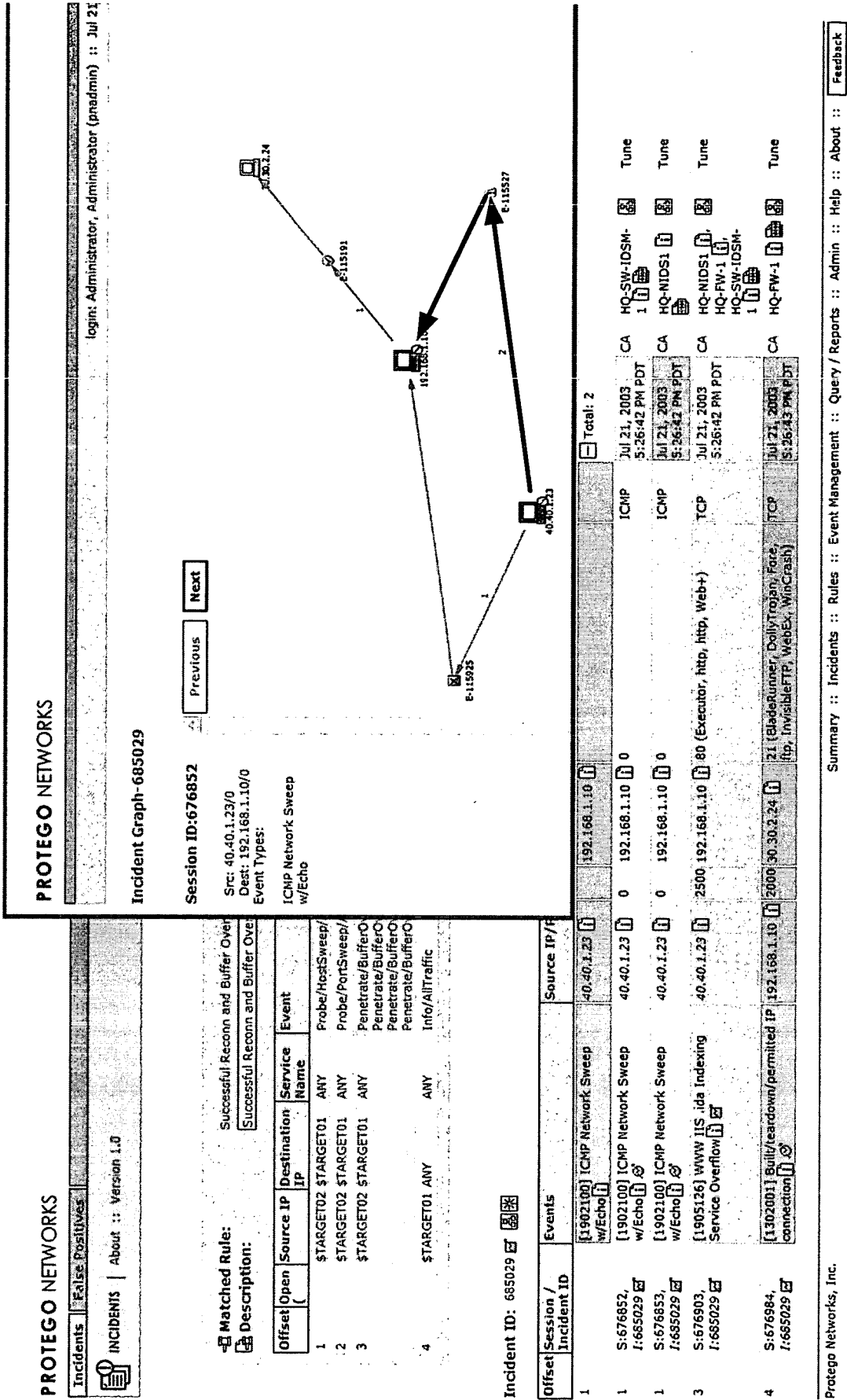


Fig. 11(B)



# PROTEGO NETWORKS

Incidents | False Positives | About :: Version 1.0

INCIDENTS | About :: Version 1.0

Logins: Administrator, Administrator (padmin) :: Jul 21, 2003 5:51:45 PM PDT :: Activate

Logout

Session ID

Raw Events - Microsoft Internet Explorer

PROTEGO NETWORKS

logins: Administrator, Administrator (padmin) :: Jul 21, 2003 5:57:01 PM PDT :: Close

ne-range

1:5mm:0ss

Escalate

Matched Rule: Successful Recon and Buffer Overflow

Description: Successful Recon and Buffer Overflow

Offset	Open	Source IP	Destination IP	Service Name	Event
1		\$TARGET02	\$TARGET01	ANY	Probe/HostSweep
2		\$TARGET02	\$TARGET01	ANY	Probe/PortSweep
3		\$TARGET02	\$TARGET01	ANY	Penetrate/Buffer
4		\$TARGET01	ANY	ANY	Info/AllTraffic

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP / Port	Destination IP / Port	Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-SW-IDS-1			Tune
1	S-676852, I-685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1			Tune
1	S-676853, I-685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1			Tune
3	S-676903, I-685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23	192.168.1.10	TCP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-FW-1			Tune
4	S-676984, I-685029	[1302001] Bullseye/heardown/permitted IP connection	192.168.1.10	2000.30.30.2.24	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1			Tune

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Fig. 12(A)



# PROTEGO NETWORKS

Incidents | False Positives

INCIDENTS | About :: Version 1.0

login: Administrator

685029

Matched Rule: Successful Recon and Buffer Overflow  
Description: Successful Recon and Buffer Overflow

Offset	Open	Source IP	Destination IP	Service Name	Event
1		\$TARGET02	\$TARGET01	ANY	Probe/HostSweep/All
2		\$TARGET02	\$TARGET01	ANY	Probe/PortSweep/All
3		\$TARGET02	\$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Penetrate/BufferOverflow/FTP, Penetrate/BufferOverflow/Mail, Penetrate/BufferOverflow/RPC, Penetrate/BufferOverflow/SSH, Penetrate/BufferOverflow/Telnet, Penetrate/BufferOverflow/Web
4		\$TARGET01	ANY	ANY	Info/AllTraffic

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP/Port	Destination IP/Port
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0
3	S:676903, I:685029	[1905126] WWW IIS .ids Indexing Service Overflow	40.40.1.23	2500 192.168.1.10 80 (Executor, http, http, Web+)
4	S:676984, I:685029	[1302001] Build/teardown/permitted connection	192.168.1.10	2000 30.30.2.24 21 (BladeRunner, DollyTrojan, Fof, InvisbleFTP, WebEx, WinCrack)

Protego Networks, Inc.

Summary :: Incidents :: Rules

Incident Graph-685029 - Microsoft Internet Explorer

## PROTEGO NETWORKS

Incident Graph-685029

Session ID:676853

Src: 40.40.1.23/0  
Dest: 192.168.1.10/0

Event Types:  
ICMP Network Sweep  
w/Echo

Previous Next

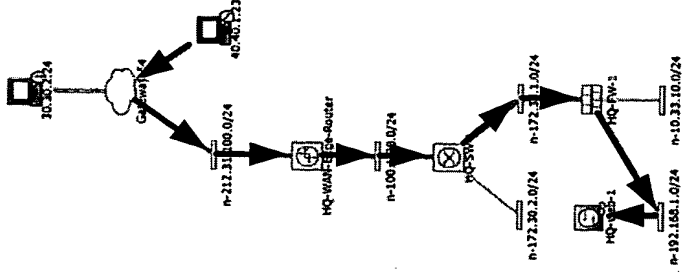


Fig. 12(B)

# PROTEGO NETWORKS

Incidents

False Positives

INCIDENTS

About :: Version 1.0

Matched Rule: Successful Recon and Buffer Over

Description: Successful Recon and Buffer Over

Offset	Open	Source IP	Destination IP	Service Name	Event
1		\$TARGET02	\$TARGET01	ANY	Probe/HostSweep/
2		\$TARGET02	\$TARGET01	ANY	Probe/PortSweep/
3		\$TARGET02	\$TARGET01	ANY	Penetrate/BufferO
4		\$TARGET02	\$TARGET01	ANY	Penetrate/BufferO
5		\$TARGET01	ANY	ANY	Info/AllTraffic

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP / R
1	S-676852 I-685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23
1	S-676853 I-685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23
1	S-676853 I-685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23
3	S-676903 I-685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23
4	S-676994 I-685029	[1302001] Built/teardown/permited IP connection	192.168.1.10

# PROTEGO NETWORKS

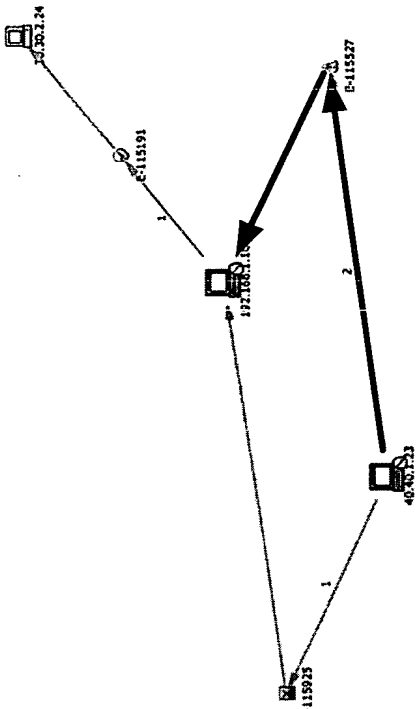
login: Administrator, Administrator (psadmin) :: Jul 21, 2003 5:26:42 PM PDT

Incident Graph-685029

Session ID: 676853

Src: 40.40.1.23/0  
Dest: 192.168.1.10/0  
Event Types:

ICMP Network Sweep w/Echo



Total: 2

Jul 21, 2003 5:26:42 PM PDT	CA	HQ-SW-IDSM-1	Tune
Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1	Tune
Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1	Tune
Jul 21, 2003 5:26:42 PM PDT	CA	HQ-FW-1	Tune
Jul 21, 2003 5:26:42 PM PDT	CA	HQ-SW-IDSM-1	Tune

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Fig. 12(C)

# PROTEGO NETWORKS

Incidents: ☒ False Positives

INCIDENTS | About :: Version 1.0

Matched Rule: Successful Recon and E

Description: Successful Recon and E

Offset	Open	Source IP	Destination IP	Service Name	Event
1		\$TARGET02	\$TARGET01	ANY	Probe/H
2		\$TARGET02	\$TARGET01	ANY	Probe/P
3		\$TARGET02	\$TARGET01	ANY	Penetrat
4		\$TARGET01	ANY	ANY	Info/Alert

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP / Port	Destination IP / Port	Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-SW-IDS-1			Tune
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1			Tune
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1			Tune
3	S:676903, I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23	2500.192.168.1.10	TCP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1, HQ-FW-1, HQ-SW-IDS-1			Tune
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10	2000.30.30.2.24	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1			Tune

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About ::

Feedback

Fig. 13(A)

# PROTEGO NETWORKS

Incidents | False Positives | About :: Version 1.0



INCIDENTS | About :: Version 1.0

login: Administrator, Admin

685029

Matched Rule: Successful Recon and Buffer Overflow  
Description: Successful Recon and Buffer Overflow

Offset	Open	Source IP	Destination IP	Service Name	Event
1		\$TARGET02	\$TARGET01	ANY	Probe/HostSweep/All
2		\$TARGET02	\$TARGET01	ANY	Probe/PortSweep/All
3		\$TARGET02	\$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Penetrate/BufferOverflow/FTP, Penetrate/BufferOverflow/Mail, Penetrate/BufferOverflow/RPC, Penetrate/BufferOverflow/SSH, Penetrate/BufferOverflow/Telnet, Penetrate/BufferOverflow/Web
4		\$TARGET01	ANY	ANY	Info/AllTraffic

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP / Port	Destination IP / Port
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0
3	S:676903, I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23	2500 192.168.1.10
4	S:676984, I:685029	[1302001] Build/teardown/permitted IP connection	192.168.1.10	2000 30.30.2.24

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Ev

## SUMMARY

Incident Graph-685029 - Microsoft Internet Explorer

## PROTEGO NETWORKS

Incident Graph-685029

Session ID:6769103

Src: 40.40.1.23/2500

Dest: 192.168.1.10/80

Event Types:

WWW IIS .ida Indexing Service Overflow

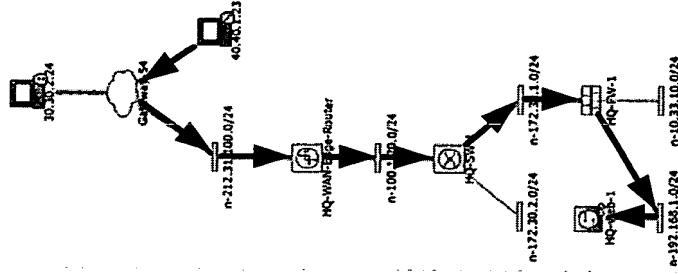


Fig. 13(B)

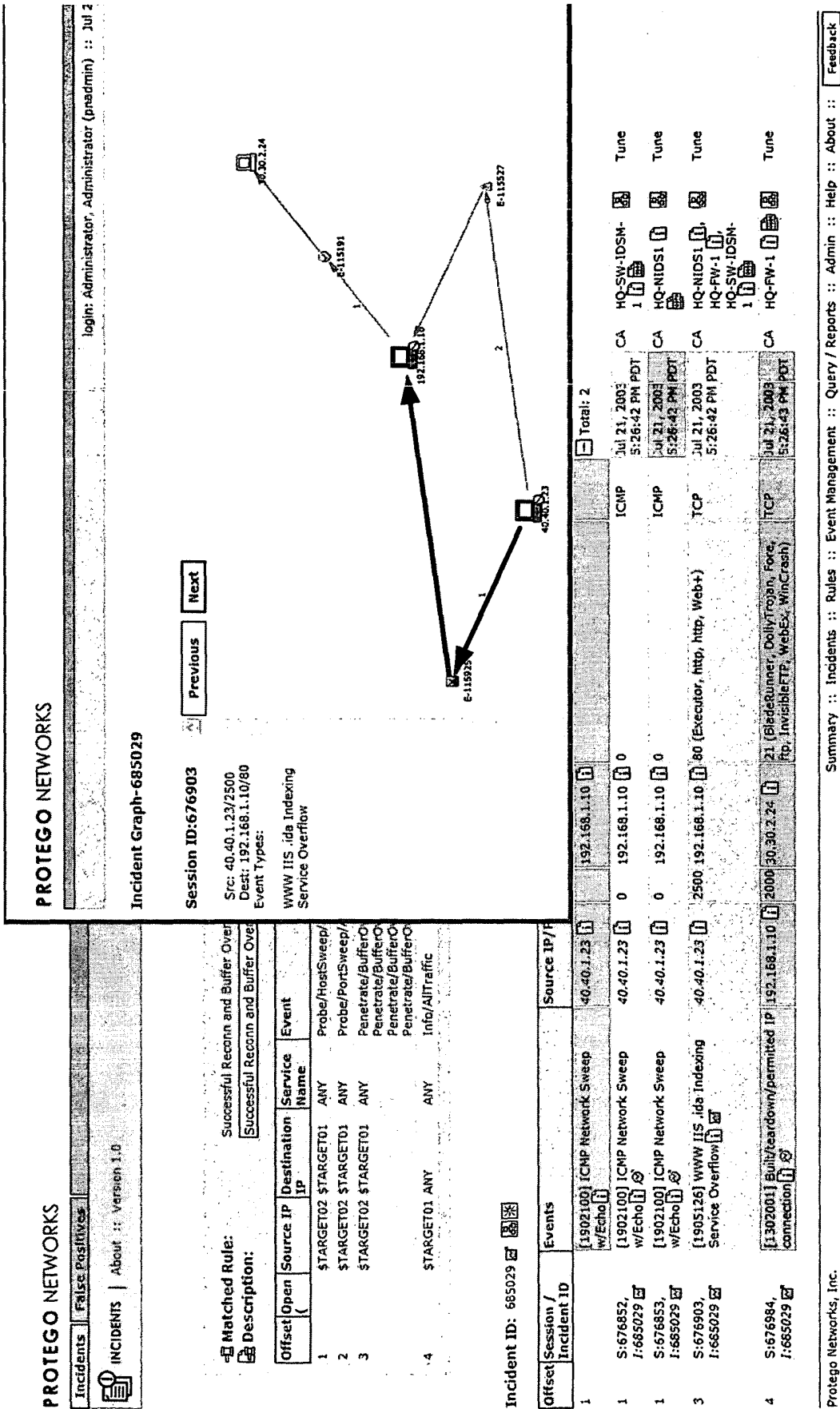


Fig. 13(C)

PROTEGO NETWORKS

Incidents | False Positives

INCIDENTS | About :: Version 1.0

Matched Rule: Successful Recon and Buffer

Description: Successful Recon and Buffer

Offset	Open	Source IP	Destination IP	Service Name	Event
1		\$TARGET02	\$TARGET01	ANY	Probe/HostSw
2		\$TARGET02	\$TARGET01	ANY	Probe/PortSw
3		\$TARGET02	\$TARGET01	ANY	Penetrate/Bufl
					Penetrate/Bufl
					Penetrate/Bufl
4		\$TARGET01	ANY	ANY	Info/AllTraffic

PROTEGO NETWORKS

Raw Events - Microsoft Internet Explorer

INCIDENTS

ABOUT

PROTEGO NETWORKS

login: Administrator, Administrator (padmin) :: Jul 21, 2003 5:58:36 PM PDT :: Close

Raw Events

Event / Session / Incident ID	Reporting Device	Time	Raw Message
E:676984, S:676984, I:685029	HQ-FW-1	Jul 21, 2003 5:26:43 PM PDT	10.33.10.2 <142>%PIX-6-302013: Built outbound TCP connection 2061 for dmz:192.168.1.10/2000 (100.1.4.1c/2000) to outside:30.30.2.24/21 (30.30.2.24/21)
E:676985, S:676984, I:685029	HQ-FW-1	Jul 21, 2003 5:26:43 PM PDT	10.33.10.2 <142>%PIX-6-302014: Tear down TCP connection 2061 for dmz:192.168.1.10/2000 to outside:30.30.2.24/21 duration 0:00:22 bytes 752 TCP Reset-O
E:676983, S:676984, I:685029	HQ-FW-1	Jul 21, 2003 5:26:43 PM PDT	10.33.10.2 <141>%PIX-6-303002: 192.168.1.10 Retrieved 30.30.2.24?url

0hh:5mm:0ss

Escalate

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP / Port	Destination IP / Port	Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-SW-IDS-1			
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1			Tune
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1			Tune
3	S:676903, I:685029	[1905126] WWW IIS .ida indexing Service Overflow	40.40.1.23	2500 192.168.1.10	TCP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-FW-1, HQ-SW-IDS-1			Tune
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10	2000 30.30.2.24	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1			Tune

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Fig. 14(A)

# PROTEGO NETWORKS

Incidents | False Positives |

INCIDENTS | About :: Version 1.0

SUMMARY

login: Administrator, Admin

685029

Matched Rule: Successful Reconnaissance and Buffer Overflow

Description: Successful Reconnaissance and Buffer Overflow

Offset	Open	Source IP	Destination IP	Service Name	Event
1		\$TARGET02	\$TARGET01	ANY	Probe/HoatSweep/All
2		\$TARGET02	\$TARGET01	ANY	Probe/PortSweep/All
3		\$TARGET02	\$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Penetrate/BufferOverflow/FTP, Penetrate/BufferOverflow/Mail, Penetrate/BufferOverflow/RPC, Penetrate/BufferOverflow/SSH, Penetrate/BufferOverflow/Telnet, Penetrate/BufferOverflow/Web
4		\$TARGET01	ANY	ANY	Info/AllTraffic

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP/Port	Destination IP/Port
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0
3	S:676903, I:685029	[1905126] WWW IIS .ida indexing Service Overflow	40.40.1.23	2500, 192.168.1.10
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10	2000, 30.30.2.24

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Ev

Incident Graph-685029 - Microsoft Internet Explorer

## PROTEGO NETWORKS

Incident Graph-685029

Session ID: 676984

Src: 192.168.1.10/2000

Dest: 30.30.2.24/21

Event Types:

Built/teardown/permitted IP connection

Previous

Next

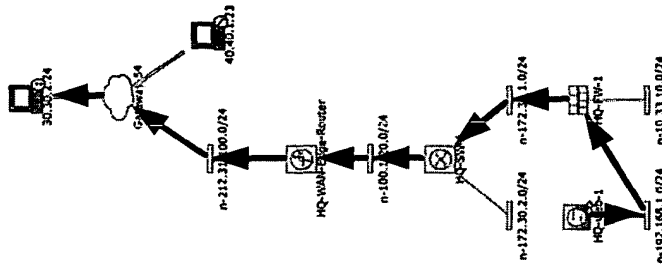


Fig. 14(B)

Session ID: 676984

Src: 192.168.1.10/2000

Src: 192.168.1.10/20  
Dest: 30.30.2.24/21

**Event Types:**

**Built/teardown/permitted IP connection**

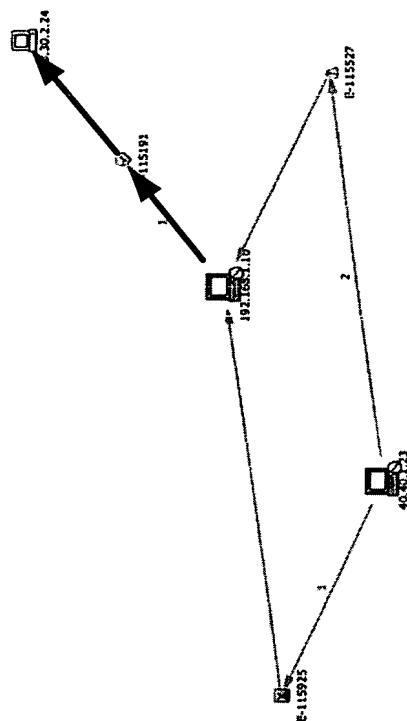
**= Matched Rule:**













**Description:**

Offset	Open	Source IP	Destination IP	Service Name	Event
1		\$TARGET02	\$TARGET01	ANY	Probe/HostSweep/
2		\$TARGET02	\$TARGET01	ANY	Probe/PortSweep/
3		\$TARGET02	\$TARGET01	ANY	Penetrate/BufferO
					Penetrate/BufferO
					Penetrate/BufferO
4		\$TARGET01	ANY	ANY	Info/AnITraffic

Incident ID: 585029  

Offset	Session / Incident ID	Events	Source IP / Port
1			
		[1902100] ICMP Network Sweep w/Echo [1]	40.40.1.23 [1]
1	S:676852, I:685029 [1]	[1902100] ICMP Network Sweep w/Echo [1] [2]	40.40.1.23 [1]
1	S:676853, I:685029 [2]	[1902100] ICMP Network Sweep w/Echo [1] [2]	40.40.1.23 [1]
3	S:676903, I:685029 [2]	[1905126] WWW IIS,ida Indexing Service Overflow [1] [2]	40.40.1.23 [1]
4	S:676984, I:685029 [2]	[1302001] Built/teardown/permitted IP connection [1] [2]	192.168.1.10 [1]



Total: 2	Jul 21, 2003	CA	HQ-SW-IDS-	Tune
	5:26:42 PM PDT		1 	
	Jul 21, 2003	CA	HQ-NIDS1	Tune
	5:26:42 PM PDT			
Total: 2	Jul 21, 2003	CA	HQ-NIDS1	Tune
	5:26:42 PM PDT		1 	
	Jul 21, 2003	CA	HQ-SW-IDS-	Tune
	5:26:42 PM PDT		1 	
Total: 2	Jul 21, 2003	CA	HQ-FW-1	Tune
	5:26:42 PM PDT		1 	
	Jul 21, 2003	CA	HQ-FW-1	Tune
	5:26:42 PM PDT		1 	

**Fig. 14(C)**





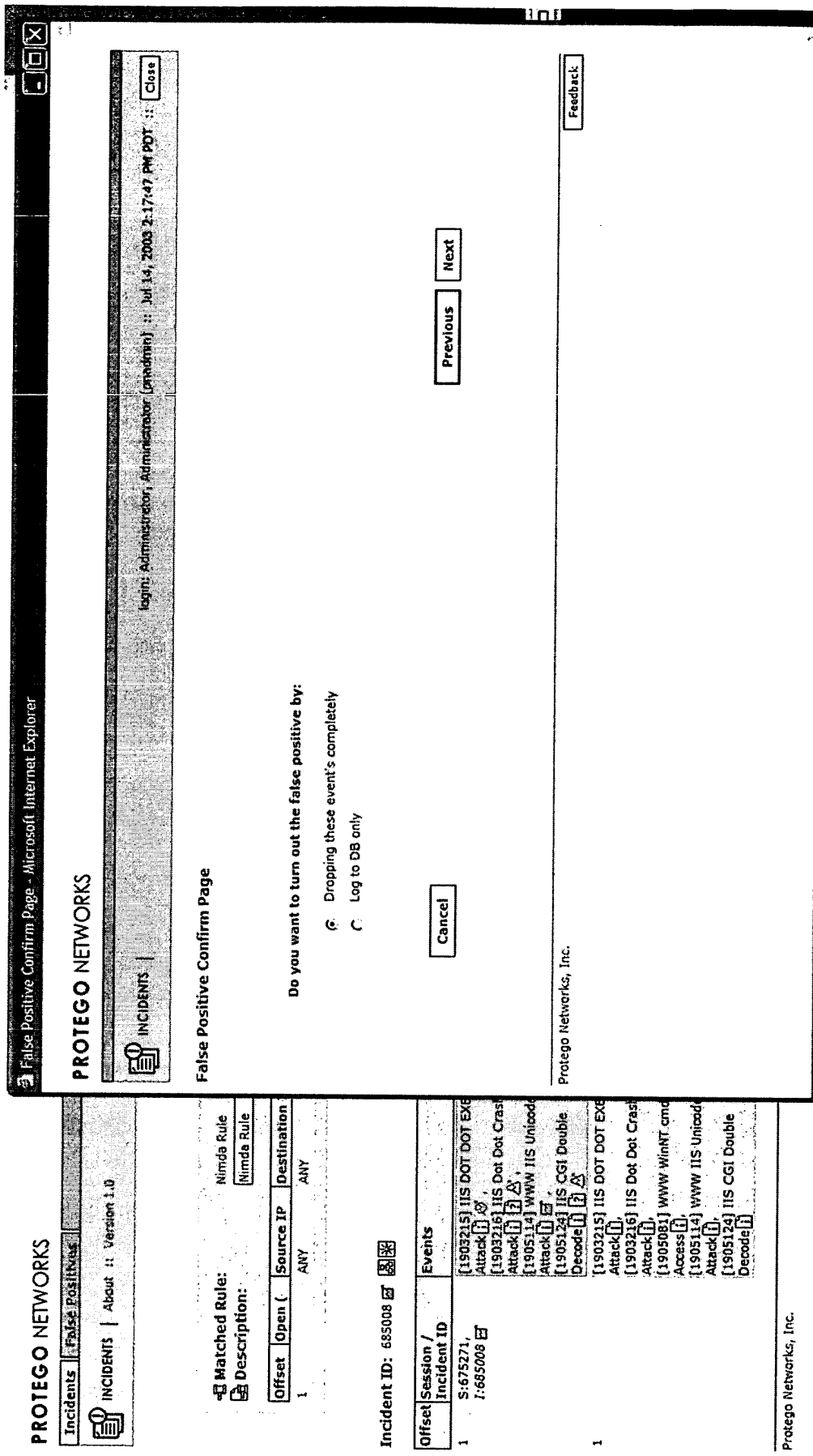


Fig. 15(B)



685008

Show Incident ID

Show Session ID

Matched Rule:  
Description:

Nimda Rule  
Nimda Rule

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Zone	Action/Operation	Time-range
1		ANY	ANY	ANY	Penetrate/Nimdaworm	ANY	ANY	5	NY	Epage	0hh:10mm:0ss

Incident ID: 685008

Escalate

Offset	Session / Incident ID	Events	Source IP / Port	Destination IP / Port	Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1	S:675271, I:685008	<div> <div>[1903216] IIS DOT DOT EXECUTE Attack</div> <div>[1903216] IIS Dot Dot Crash Attack</div> <div>[1905114] WWW IIS Unicode Attack</div> <div>[1905124] IIS CGI Double Decode</div> <div>[1903216] IIS DOT DOT EXECUTE Attack</div> <div>[1903216] IIS Dot Dot Crash Attack</div> <div>[1905081] WWW WinNT cmd.exe Access</div> <div>[1905114] WWW IIS Unicode Attack</div> <div>[1905124] IIS CGI Double Decode</div> <div>Total: 5</div> </div>	20.20.1.15	172.29.99.21	TCP	Jul 14, 2003 2:00:57 PM PDT	CA	HQ-NIDS-2 HQ-FW-2 HQ-SW-IDSN-1			Tune

Fig. 15(D)



Incidents
False Positives
INCIDENTS
About :: Version 1.0
login: Administrator, Administrator (pnaadmin) :: Logout
10/14/2003 2:22:02 PM PDT :: Activate

Select False Positive: Confirmed False Positive Type

Count	Incidents	Event	Destination IP/Port	Protocol	Zone
7	I:415004 <input checked="" type="checkbox"/> , I:415008 <input checked="" type="checkbox"/> , I:550001 <input checked="" type="checkbox"/> , I:550008 <input checked="" type="checkbox"/> , I:550012 <input checked="" type="checkbox"/> , I:685004 <input checked="" type="checkbox"/> , I:685008 <input checked="" type="checkbox"/>	[1903216] IIS Dot Dot Crash Attack <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	172.29.99.21 <input checked="" type="checkbox"/>	80 TCP	CA
5	I:415004 <input checked="" type="checkbox"/> , I:415008 <input checked="" type="checkbox"/> , I:550001 <input checked="" type="checkbox"/> , I:550008 <input checked="" type="checkbox"/> , I:550012 <input checked="" type="checkbox"/>	[1905081] WWW WinNT cmd.exe Access <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	172.29.99.21 <input checked="" type="checkbox"/>	80 TCP	CA

1 to 2 of 2 25 per page

Change Status

Protego Networks, Inc.
Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Fig. 16(B)

Matched Rule:  
Description:

Nimda Rule  
Nimda Rule

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Zone	) Close	Action/Operation	Time-range
1		ANY	ANY	ANY	Penetrate/Nimdaworm	ANY	ANY	5	NY		Epage	0hh:10mm:0ss

Incident ID: 685008

Escalate

Offset/Session / Incident ID	Events	Source IP/Port	Destination IP/Port	Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1 S:675271, I:685008	[1903215] IIS DOT DOT EXECUTE Attack [1903215] IIS Dot Dot Crash	20.20.1.15	172.29.99.21	TCP	Jul 14, 2003 2:00:57 PM PDT	CA	HQ-NIDS-2 [1903215] HQ-FW-2 [1903215] HQ-SW-IDSN-			Tune

Query - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media

Address http://10.1.1.129:8080/gul/Query/index.jsp

Free Downloads Downloads Options

PROTEGO NETWORKS

Query Report

QUERY / REPORTS | About :: Version 1.0

login: Administrator, Administrator (nadmin) :: Logout :: Jul 14, 2003 2:32:05 PM PDT :: Activate

1701

Show Incident ID

Show Session ID

Query Event Data

Click the cells below to change query criteria:

Source IP	Destination IP	Service	Events	Device	Severity	Zone	Operation	Rule	Action	Time Range	Display Format
20.20.1.15	ANY	ANY	ANY	ANY	ANY	ANY	None	ANY	ANY	1hh:0mm:0ss	Sessions

Save As Report

Save As Rule

Clear

Submit

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Protego Networks, Inc.

Fig. 17(A)

Fig. 17(B)



Fig. 17(C)